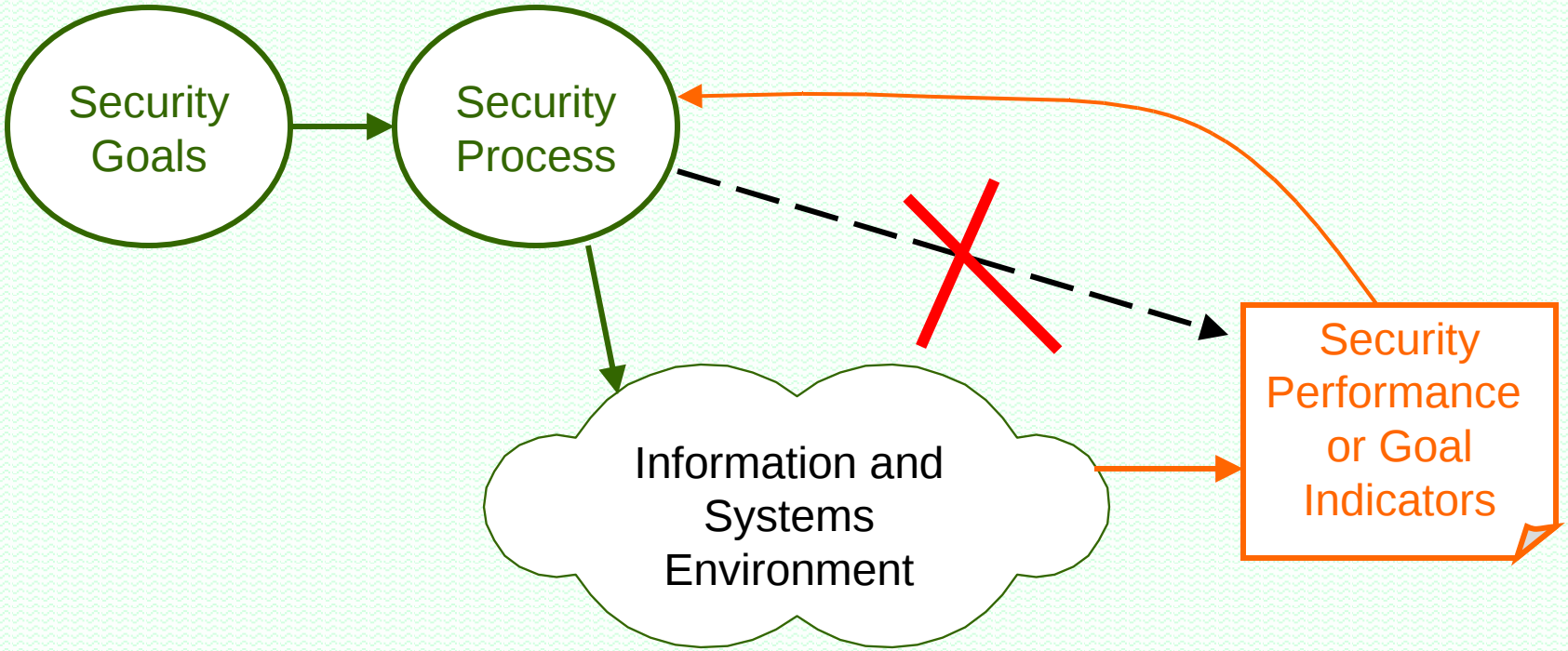
Sine Qua Non

Jennifer Bayuk, CISA, CISM, CGEIT

Independent Information Security Consultant

www.bayuk.com

Security Metrics



Map to Program Objectives

Maps linking metrics to InfoSec program objectives are based on the relationship of a process to an objective and are defined by the attributed of each people, process, or technology component. Maps may be based on any data source, including:

- Logs
- Configurations
- Services
- Tasks
- Surveys

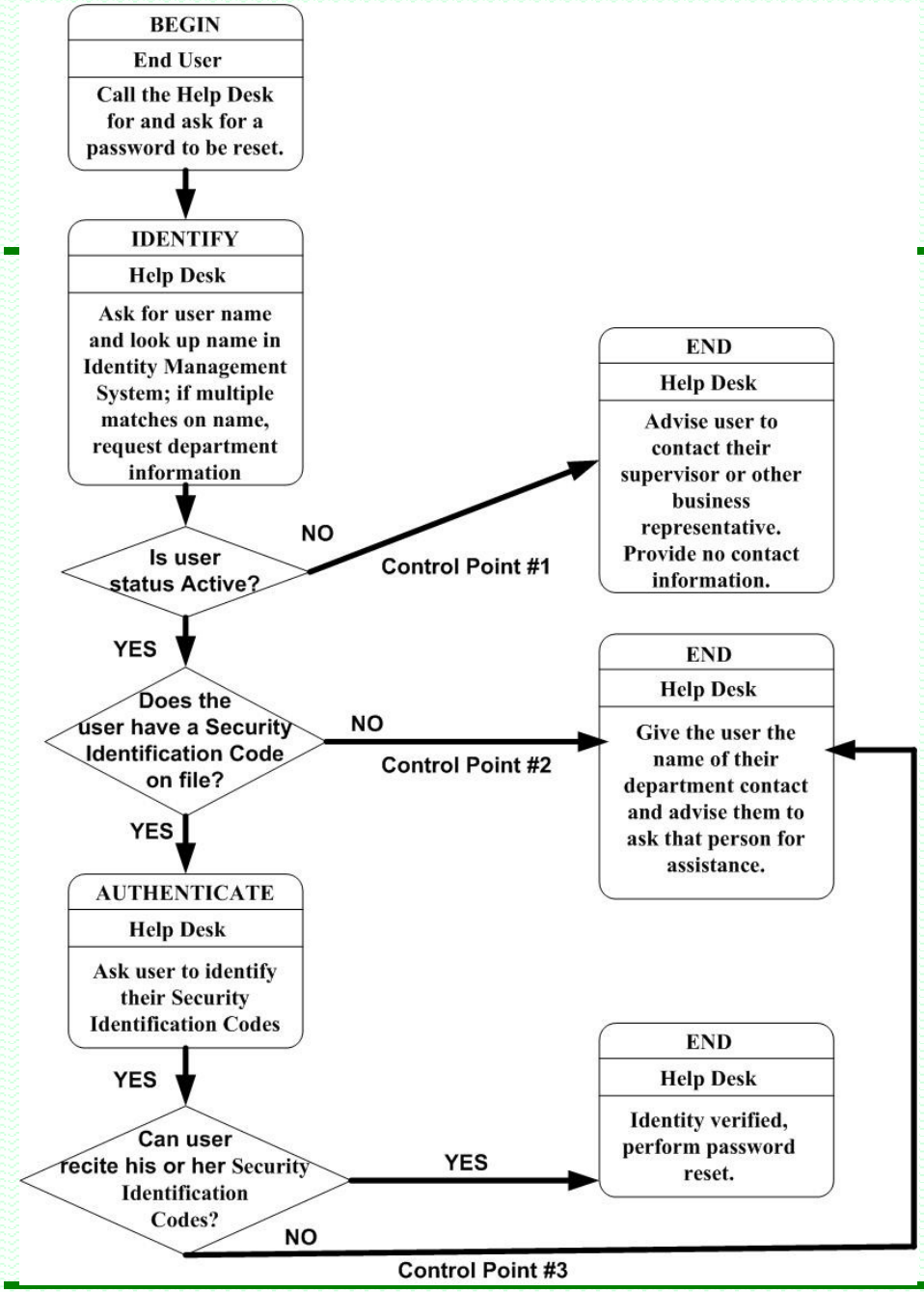
Types of Metrics

A - Activity Related Metric: Metrics that Measure Work Activity

T - Target Related Metric: Metrics that Have a Measurable target (i.e. No Missing Logs)

R – Remediation Metric: Metrics that Show Progress toward a Goal

M - Monitor Related Metric: Metrics that Monitor Processes



Example

A – Number of calls related to password reset.

T – Percent of user records that have a security identification code on file

R – Number of user accounts hijacked via unauthorized password reset.

M – For each staff member, percent of password reset calls where staff followed (and/or documented) process.

Focus on Target: What is 100%

User: Identity Management

System: Hardware Inventory

Application: Component Mapping

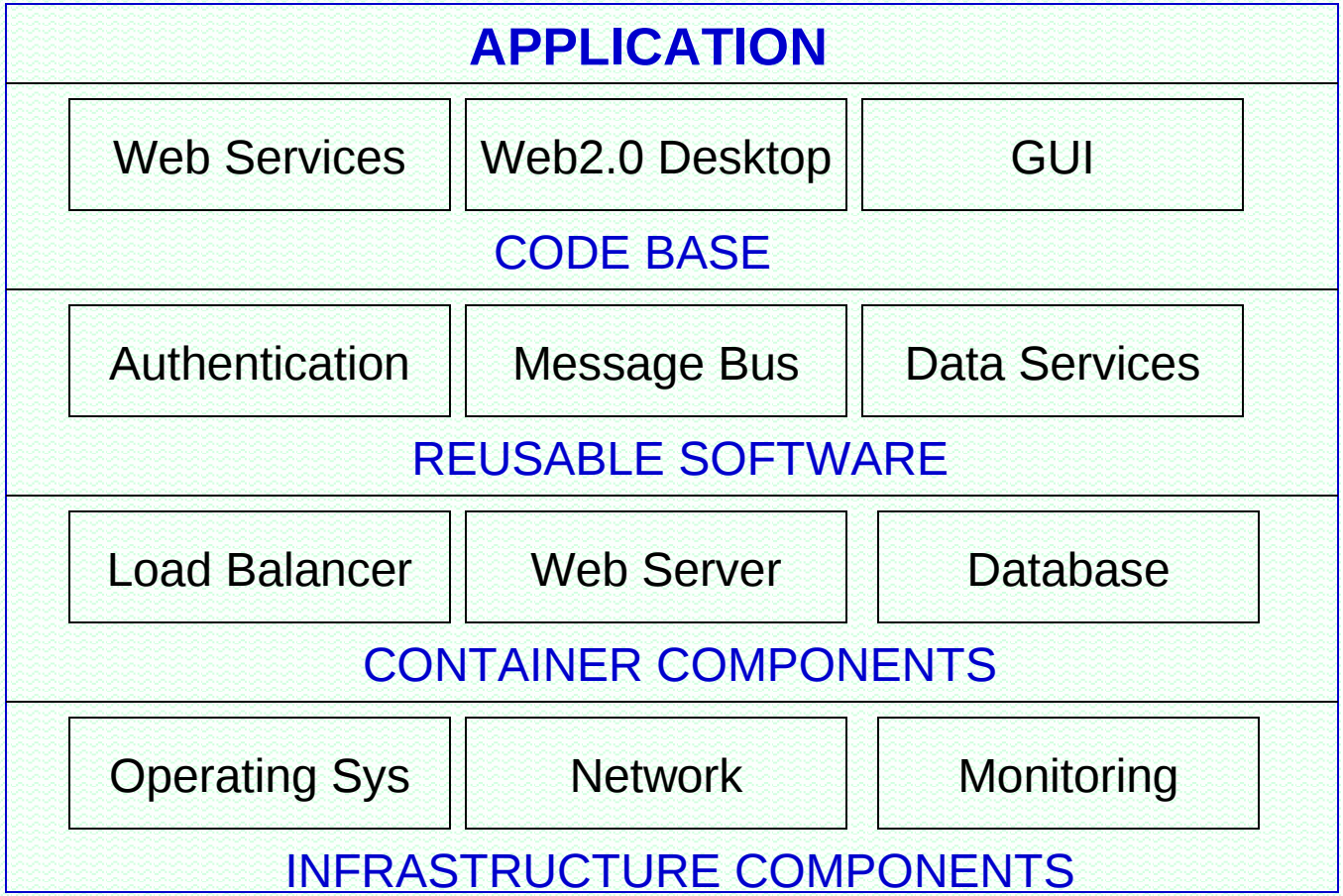
Data: Information Classification

No target metrics have credibility unless there is a definition of 100%.

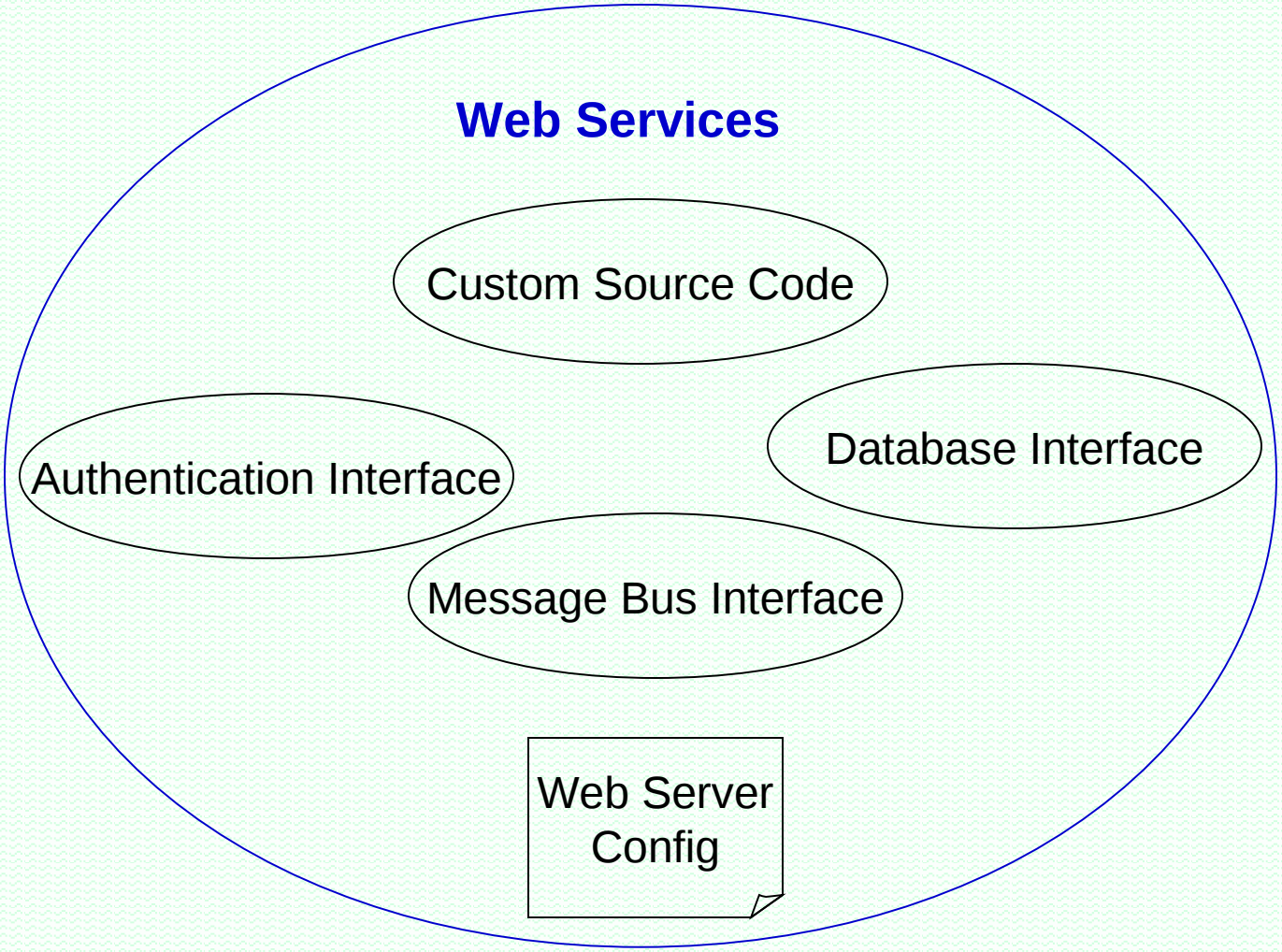
Focus on Applications

- Source code to component
- Component to software configuration
- Component to hardware platform
- Component to network service

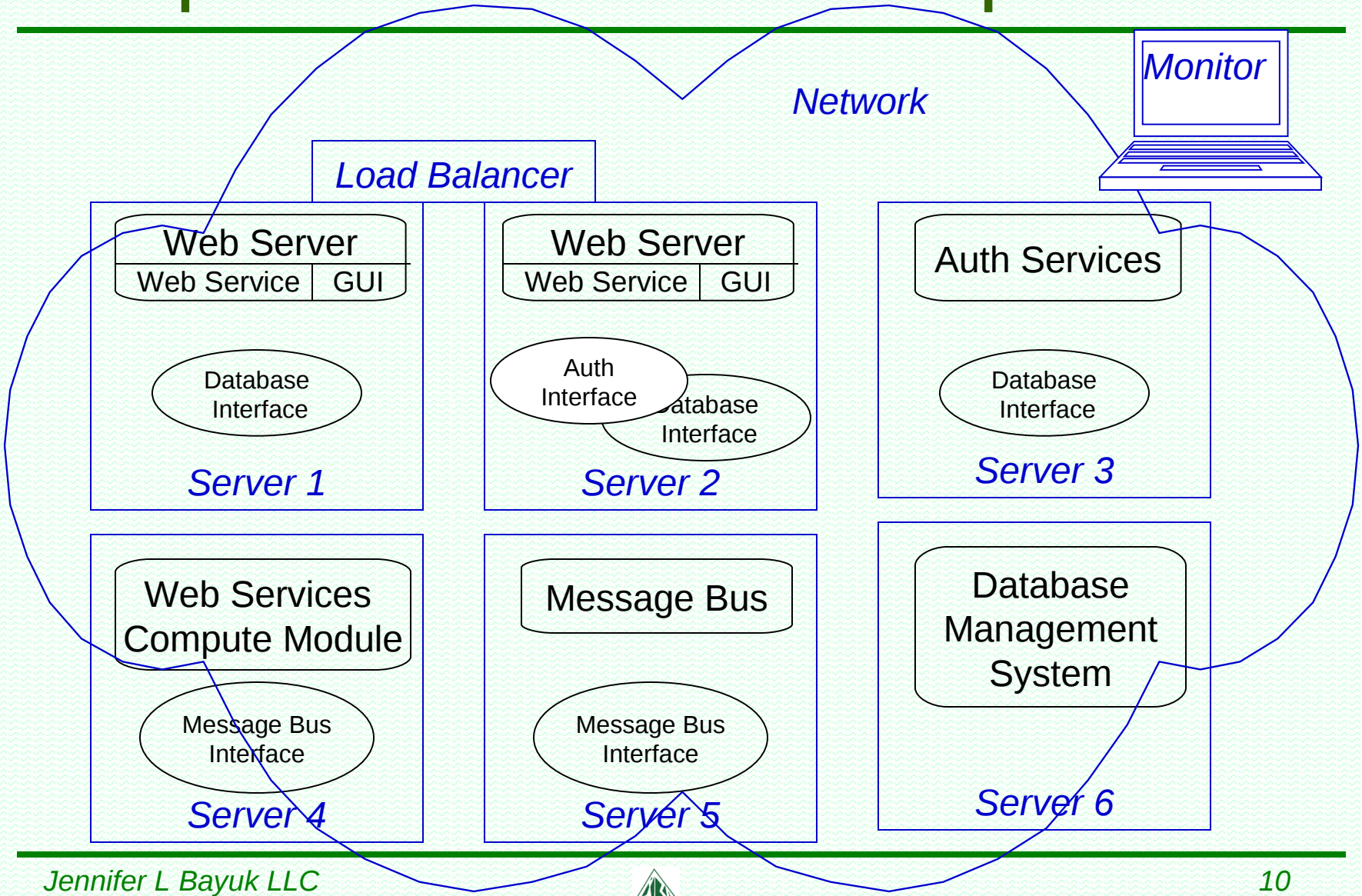
Application components



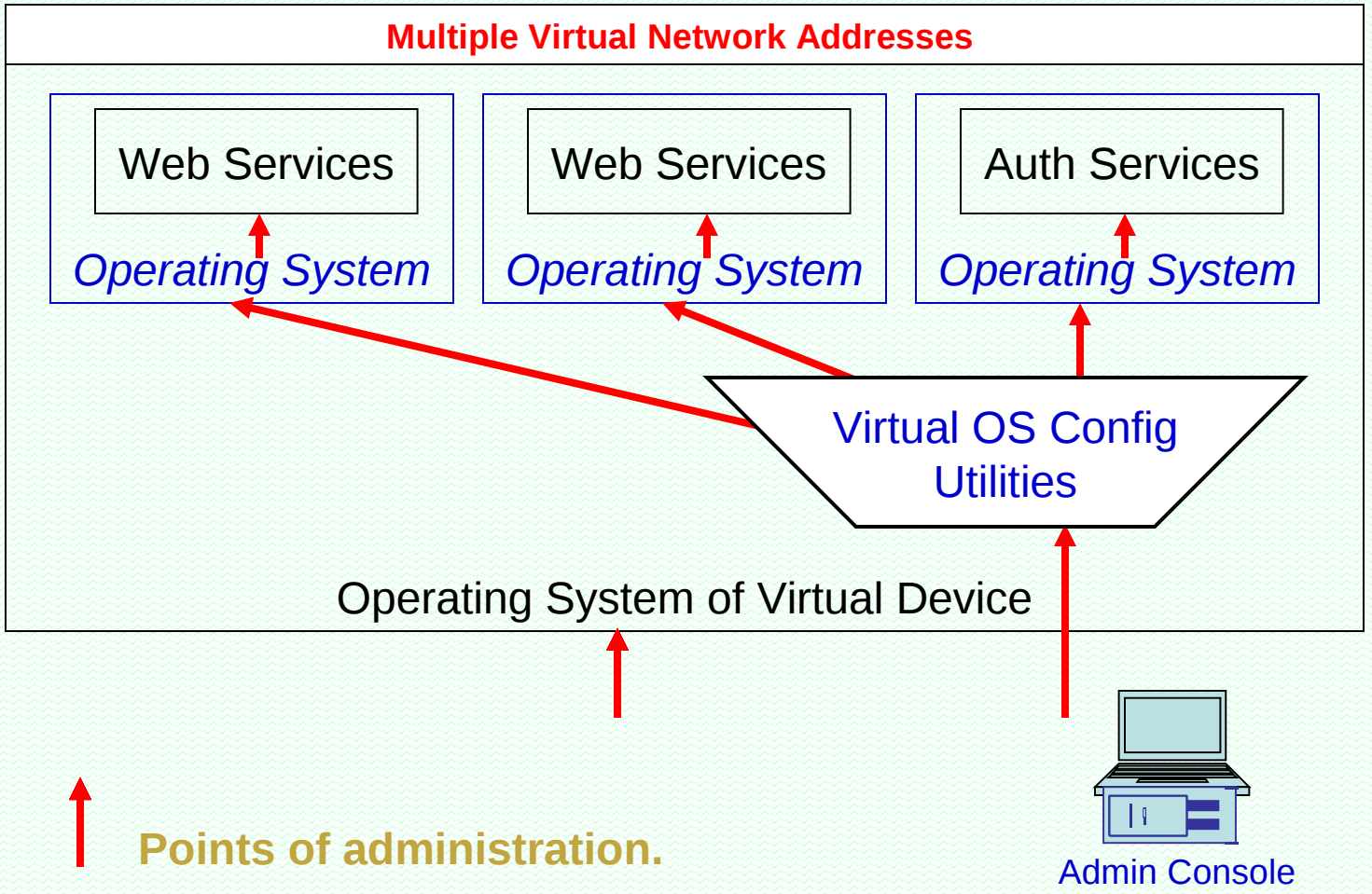
Component to software config



Component to hardware platform



Virtual Machine Complications

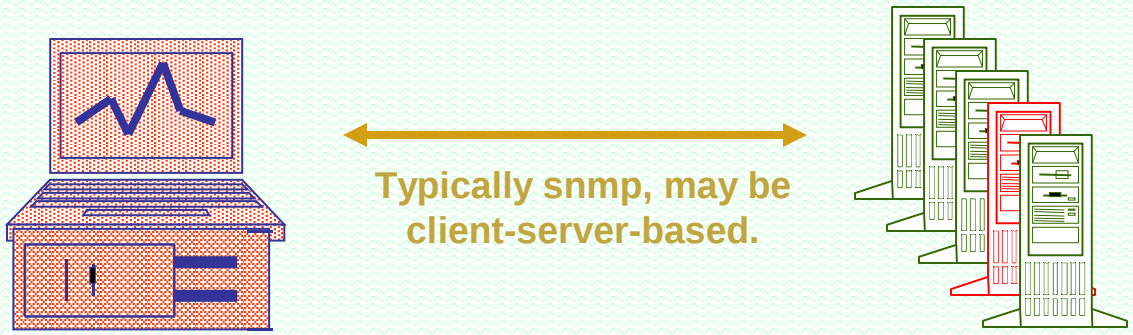


Potential Data Sources

- Enterprise Management System
- Configuration Management Database
- Application Inventory

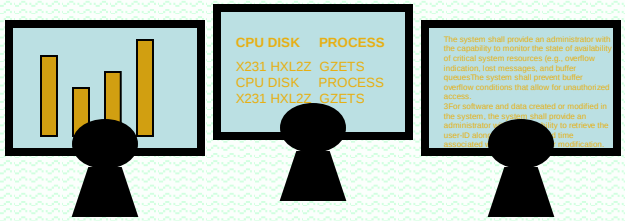
Enterprise Management System

- IP centric asset inventory
- OS and Infrastructure focused
- Requires coordinated data entry or feeds to align with business process



Configuration Management DB

- Operations focused
- Provides relationships between configuration items
- Requires coordinated data entry or feeds to align with asset inventory and/or business process



Typically used to support operations and service desk.

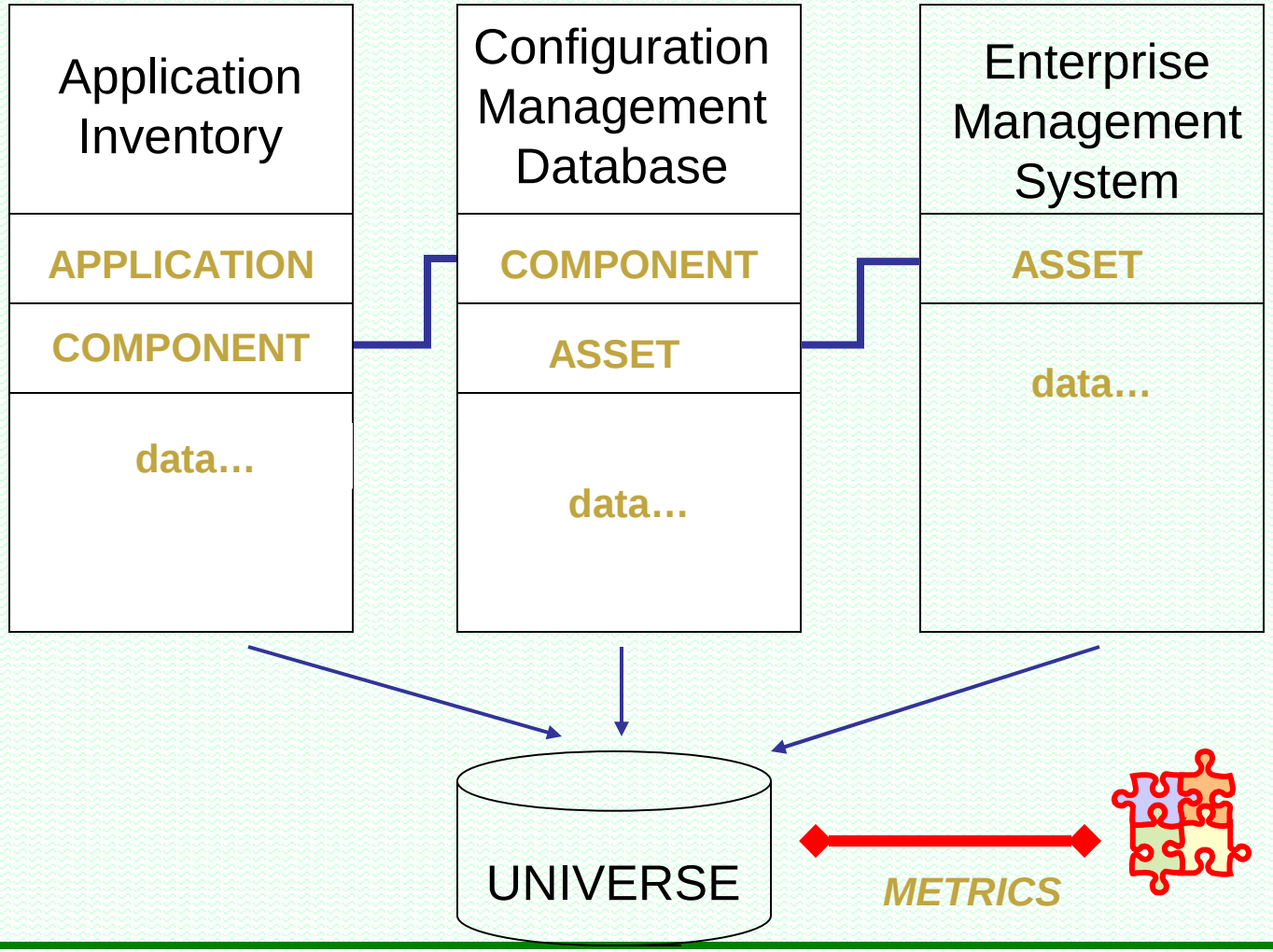
Application Inventory

- Development focused
- Provides accountability for maintenance of software
- Requires coordinated data entry or feeds to align with asset inventory

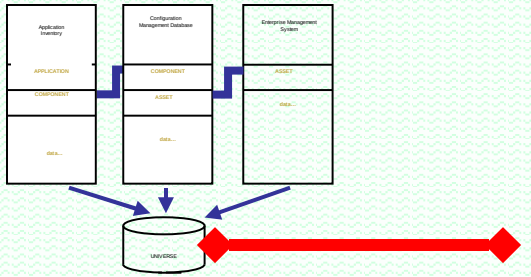
Acronym	MGR	DEPT	Components
APPACRO	Smith, Deb	Legal & Comp	Web
SALES	Jones, John	Sales Services	Mainframe
FINANC	Mathews, David	Enterpr Finance	SAP
MARKET	Edison, James	Sales and Market	Web
MGMTAPP	Johnson, Kelly	Network Mgmt	Desktop
OTHAPP	Williams, Peter	Corp & Admin	Mini

Typically used to justify IT Spend to Business Customers.

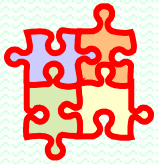
Data Source Consolidation



Link Indexes to Security Data



From *Data Consolidation* slide



Control Attributes

APPLICATION

IMPACT

BCP Data

Accountability Attributes

COMPONENT

IT Manager

Support team

Security Review Database

Identity Management Database

Common Indexes cannot be expected to exist in different realms and different management domains.

Expectations for linkage must be articulated.

Potential Security Process Links

1. Security Software Configuration
2. Change Authorization Correlation
3. Security Review or Audit Scope
4. Information Classification
5. Outsourcing Arrangements
6. Application Impact
7. Business Recovery Objectives
8. System Development Projects

Potential accountability links

1. Line of Business
2. Development Team Acronym
3. IT Manager Realm of Responsibility
4. Support Escalation Chain
5. Identity Management System

Typical Gaps

1. Application Index or Acronyms
   - e.g.: without associated equipment
2. Vendor Software Release Identifier
   - e.g.: not associated with any application
3. Network IP Address
   - e.g.: with no equipment serial numbers
4. Equipment Serial Number
   - e.g.: not associated with any vendor

Conclusion

Not only is it possible to specify minimum datasets that are required to maintain security,

it is a necessary (though not sufficient) requirement to produce any other security metric.